

AO-106 (Rev. 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the
Northern District of Oklahoma

In the Matter of the Search of
Information Associated with accounts colby.mcginis.737
and bdclement that is Stored at a Premises Controlled by
Meta Platforms, Inc.

Case No. 22-mj-815-SH
FILED UNDER SEAL

FILED
DEC 21 2022Mark C. McCart, Clerk
U.S. DISTRICT COURT

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §1343
18 U.S.C. §1344
18 U.S.C. §1028A

Wire Fraud
Bank Fraud
Aggravated Identity Theft

The application is based on these facts:

See Affidavit of David Brydie attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

SA David Brydie, USSS
Printed name and title

Sworn to before me by phone.

Date: 12/21/22City and state: Tulsa, Oklahoma


Judge's signature

Susan E. Huntsman, U.S. Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with Facebook
accounts colby.mcgininis.737 and
bdclement that is Stored at a Premises
Controlled by Meta Platforms, Inc.**

Case No. _____

FILED UNDER SEAL

Affidavit in Support of an Application for a Search Warrant

I, David Brydie, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with the Facebook accounts: **bdclement** and **colby.mcgininis.737** (together the “**TARGET ACCOUNTS**”) that is stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the **TARGET ACCOUNTS**, as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-

authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Secret Service (USSS) and have been since August 2019. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, as well as other violations of federal law. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. I am an investigative and law enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of Title 18, United States Code, Section 3056. As a result of my personal participation in the investigation of matters discussed in this affidavit, I am familiar with the facts and circumstances of this case. The facts and circumstances discussed below were derived through my examination of records, my conversation with other law enforcement officers, various other sources of information, and through my knowledge, experience and training.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on knowledge obtained from other law enforcement officers, my review of documents related to this investigation,

conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Facebook account contains: evidence of violations of Title 18, United States Code § 1343 (Wire Fraud), Title 18, United States Code § 1344 (Bank Fraud), Title 18, United States Code § 1028A (Aggravated Identity Theft) (collectively, the “TARGET OFFENSES”) by Colby Howard McGinnis.

Jurisdiction

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally,

the government may obtain an order precluding Meta from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Meta Background

7. Meta owns and operates Facebook, a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

8. Meta asks Facebook users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

9. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange

communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

10. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

11. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user

and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

12. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can “tag” other Facebook users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

13. Facebook users can use Facebook Messenger to communicate with other users via text, voice, and video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and also retains transactional records related to voice and video chats, including the date of each call. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

14. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

15. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

16. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

17. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

18. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

19. Facebook also offers Facebook Pay (now called Meta Pay)¹, which it describes as a seamless and secure way for users to make payments on Facebook, Messenger, Instagram, and in participating online stores. After a user provides your payment card or account information, they can use Facebook Pay (Meta Pay) to make purchases, send money, donate within the apps, or check out when shopping online.

¹ According to Facebook's website, Facebook Pay is now called Meta Pay, and the name change will "roll out globally over time." See <https://www.facebook.com/help/1434403039959381>.

20. In addition to the applications described above, Meta provides users with access thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that user’s access or use of that application may appear on the user’s profile page.

21. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user’s IP address is retained by Meta along with a timestamp.

22. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables “Location History,” “checks-in” to an event, or tags a post with a location.

23. Social networking providers like Meta typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Meta typically retains records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may

provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, Meta's servers are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

26. On December 2, 2022, Detective Shaw of the Tulsa Police Department previously requested that Meta preserve any information for the accounts listed in Attachment A.

Probable Cause

The Unauthorized Transactions

27. On November 21, 2022, Detective Robert Shaw of the Tulsa Police Department was assigned to investigate a report initiated by victim M.B. M.B. informed Detective Shaw that she ordered a debit card ending in 4061 from Arvest Bank, and the card was mistakenly sent to her previous address in Tulsa 1641, East 31st, Street, Tulsa, Oklahoma. Arvest Bank is, and at all times pertinent to this affidavit was, insured by the Federal Deposit Insurance Corporation.

28. M.B. informed Detective Shaw that she never received the card because she currently lives in Colorado. M.B. stated she became aware that between November 3, 2022, and November 18, 2022, her debit card had been used without her authorization for approximately \$15,000 worth of charges at various retail locations in and around the Tulsa, Oklahoma, area.

29. Detective Shaw contacted Isaac Velasquez of Arvest Bank who provided him with a ledger of purchases made on M.B.'s card. The ledger shows multiple transactions on the card at QuikTrip locations in the Tulsa area. Detective Shaw subsequently obtained surveillance footage for the date and times of the disputed transactions from QuikTrip. Of note, the surveillance footage and transaction ledger reviewed together show as follows:

- a. On November 3, 2022, at approximately 10:44 pm CT, M.B.'s card ending in 4061 was used at the Burlington Coat Store for the purchase of miscellaneous items totaling approximately \$928.40. Surveillance footage obtained from Burlington Coat Store from that date and time shows a white male with neck tattoos and a blond woman. The white male in the footage is shown completing the transaction with the cash register and presenting a card for payment. A sample still photo from the surveillance obtained from that date and approximate time is provided below:



- b. On November 4, 2022, at approximately 1:03 AM CT, M.B.'s card ending in 4061 was used at the QuikTrip located at 3008 E. 11th Street, Tulsa, Oklahoma, for \$45.83. The surveillance footage for that date and approximate time shows a white male with neck tattoos and a blond woman. The white male subject is seen inserting the card into the POS machine and walking out with the merchandise. A still photo of the surveillance footage is provided below:



- c. On November 5, 2022, at approximately 2:18 AM CT M.B.'s card ending in 4061 was used at QuikTrip located at 3008 E. 11th Street in Tulsa, Oklahoma for \$502.50. The surveillance footage from that location for that date and time shows a white male in a dark jacket standing at the ATM and using a debit card. The individual appears to be the same male from the previous footage. The male subject is seen inserting the card into the ATM machine and walking out with the withdrawn cash. A still photo of the surveillance footage is provided below:



- d. On November 6, 2022, at approximately 3:20 pm CT, M.B.'s card ending in 4061 was used at the QuikTrip located at 3008 E. 11th Street, Tulsa, Oklahoma, for \$502.50. The surveillance footage from that incident shows a white male in a white jacket standing at the ATM and using the card. From the footage, the male appears to have the same distinctive tattoos on the subject's neck and left arm as the individual previously seen at Burlington. A still photo of the surveillance footage is provided below:



- e. On November 7, 2022, between approximately 1:05 am and 1:07 am, M.B.'s card ending in 4061 was used multiple times at the QuikTrip located at 3008 E. 11th Street, Tulsa, Oklahoma for ATM transactions in the amounts of \$502.50, \$302.50, and \$202.50 respectively. The surveillance footage shows a white male in a white jacket standing at the ATM and using a debit card. The male is seen inserting the card into the machine and walking out with the withdrawn cash on his way out, and a tattoo is visible on his left hand. A still photo of the surveillance footage is provided below:



- f. On November 9, 2022, at approximately 2:54pm CT and 2:55pm CT M.B.'s card ending in 4061 was used at the QuikTrip located at 1509 S. Lewis Ave, Tulsa, Oklahoma for two separate transactions each in the amount of \$502.50. The surveillance footage shows a white male with a red hoodie and a blonde woman with an orange jacket. The white male subject is seen inserting the card into the ATM machine and walking out with cash.

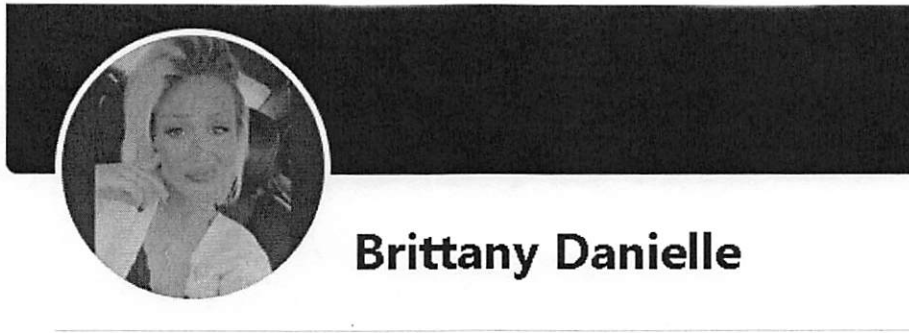


The Facebook Transactions

30. Records obtained from Arvest showed that over \$1,000 of the account funds were sent through various transactions via Facebook. Samples of the Facebook transactions appearing in the account records are provided below:

<u>Date</u>	<u>Amount</u>	<u>Merchant/Location</u>
FACEBOOK.COM 650-543-7818, CA US	\$275 CR	FACEBOOK.COM 650-543-7818, CA US
11/3/2022	\$500 DR	FBPAY *Brittany Danie pay.fb.com, CA US
11/3/2022	\$300 DR	FBPAY *Brittany Danie pay.fb.com, CA US
11/4/2022	\$275 DR	FBPAY *Brittany Danie pay.fb.com, CA US

31. Detective Shaw conducted a searched for Tulsa area Facebook accounts using the search query Britany Danie and identified the account **bdclement**, with the user profile of Brittany Danielle. A screenshot for the profile appearing on the webpage associated with this account is provided below.



32. On the page for this **bdclement** account, Detective Shaw observed a blonde woman with a white male who had distinct neck tattoos and tattoo sleeves on his arms which appear to match the individual seen in the aforementioned surveillance. After reviewing the page for the account, Detective Shaw observed a male in the photos with unique neck tattoos.

33. Detective Shaw proceeded to review Brittany Danielle's Facebook friends on her account and was able to identify what appeared to be the account of the male he had identified in the photographs of Brittany Danielle's page, which appears to belong to a white male named Colby McGinnis, with account name **colby.mcginnis.737**. A screenshot of the **colby.mcginnis.737** account is provided below:



34. Detective Shaw ran the names Colby McGinnis and Brittany Danielle in TPD's database and identified: Colby McGinnis, DOB: xx/xx/1991 and Brittany Danielle Clement, DOB: xx/xx/1993. Detective Shaw pulled McGinnis' DOC#659169 information and accompanying booking photo, which is provided below.



35. Detective Shaw further contacted TPD Officer N. Cantrell, who had face to face contact with Colby McGinnis during a traffic stop conducted on June 14, 2022, which was recorded on body worn camera. Officer Cantrell reviewed the

surveillance stills discussed in this affidavit and stated he could testify the individual from the surveillance was the Colby McGinnis with whom he had contact on the evening of June 14, 2022.

36. Detective Shaw contacted the Cherokee Nation who stated that Mr. McGinnis is a member of their tribe, with citizen ID # 346736.

Information to be Searched and Things to be Seized

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

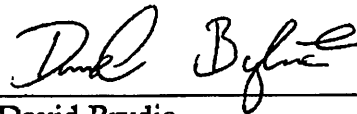
39. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

40. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of the TARGET OFFENSES associated with the TARGET ACCOUNTS described in Attachment A.

41. I request to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "David Brydie", written over a horizontal line.

David Brydie
Special Agent
United States Secret Service

Subscribed and sworn to by phone on December 21st, 2022.

A handwritten signature in cursive script, appearing to read "Susan E. Huntsman", written over a horizontal line.

SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the Facebook accounts named **bdcllement** and **colby.mcgininis.737** (the “TARGET ACCOUNTS”) that is stored at a premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the TARGET ACCOUNTS, including:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
2. All information relating to the TARGET ACCOUNTS’ association or use of Facebook Pay (Meta Pay), or any other payment application accessible through Facebook, including, but not limited to, all accounts and methods of payment linked to the TARGET ACCOUNTS, and all monetary transactions involving the TARGET ACCOUNTS.

3. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
4. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
5. All IP logs, including all records of the IP addresses that logged into the account;
6. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
7. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
8. All past and present lists of friends created by the TARGET ACCOUNTS;
9. The types of service utilized by the user;

10. All associated logs and metadata;

B. All content, records, and other information relating to communications sent from or received by the **TARGET ACCOUNTS** from **11/1/2022 to the present**, including but not limited to:

1. All Facebook Pay (Meta Pay) transactions and all information regarding any transaction or activity requiring payment of any form, including all information relating to the manner and method of payment for any such transaction;
2. The content of all communications sent from or received by the **TARGET ACCOUNTS**, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content, if available;
3. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
4. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
5. All other records and contents of communications and messages made or received by the user including all Messenger activity, private

messages, chat history, video and voice calling history, and pending
“Friend” requests;

6. All “check ins” and other location information;
7. All records pertaining to communications between Meta and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken;

C. All content, records, and other information relating to all other interactions between the TARGET ACCOUNTS and other Facebook users, including but not limited to:

1. All financial transactions between the account of any type, including but not limited to any and all Facebook Pay (Meta Pay) transactions, and any all methods of payment used for same;
2. All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
3. All information about the user’s access and use of Facebook Marketplace;
4. All information about the Facebook pages that the account is or was a “fan” of;

D. All records of Facebook searches performed by the TARGET ACCOUNTS;

E. All location information, including location history, login activity, information geotags, and related metadata.

Meta is further ordered to disclose the above information to the government within 14 days after service of this warrant.

II. Information to be searched for and seized by the government

All information described above in Section I that constitutes evidence and/or fruits of violations Title 18, United States Code § 1343 (Wire Fraud), Title 18, United States Code § 1344 (Bank Fraud), and Title 18, United States Code § 1028A (Aggravated Identity Theft) (collectively, the “TARGET OFFENSES”), including, for each TARGET ACCOUNT or identifier listed on Attachment A:

- a. All information relating to the TARGET ACCOUNTS’ association or use of Facebook Pay (Meta Pay), or any other payment application accessible through Facebook, including, but not limited to, all accounts and methods of payment linked to the TARGET ACCOUNTS, and all monetary transactions involving the TARGET ACCOUNTS that relate to the TARGET OFFENSES, or that relate to money or property obtained through commission of the TARGET OFFENSES;
- b. Communications between the TARGET ACCOUNTS and others relating to the TARGET OFFENSES, or relating to money or property obtained through commission of the TARGET OFFENSES;

- c. Evidence indicating how and when the TARGET ACCOUNTS were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the TARGET OFFENSES under investigation and to the Facebook account owner;
- d. Evidence indicating the TARGET ACCOUNT owner's state of mind as it relates to the TARGET OFFENSES under investigation;
- e. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. (“Meta”) and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of account records associated with the Facebook accounts bdclement and colby.mcginnis.737. I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. Such records were generated by Meta’s electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature